Глава 5

Нелинейни диофантови уравнения.

Дефиниция 5.0.1 *Нелинейно диофантово уравнение с две неизвестни се нарича уравнение от вида*

$$f(x,y) = 0,$$

чиито решение търсим в цели числа, където $f(x,y)$ е полином на x и y с цели коефициенти и степен поне две. Ако търсим решението в $\mathbb{Z}_n$, то казваме, че решаваме диофантово сравнение по модул n.

Да отбележим, че ако горното уравнение има решение в цели числа, то трябва да има решение и по модул всяко просто число p, т.е. в $\mathbb{Z}_p$. Този факт позволява да се доказва нерешимост на уравнението - ако се намери p, такова че в $\mathbb{Z}_p$ няма решение, то няма да има решение и в цели числа.

В настоящите лекции ще се спрем само на уравненията от втора степен.

5.1 Диофантови уравнения от втора степен.

Всяко диофантово уравнение от втора степен с две неизвестни може да се запише (след евентуално умножаване с 2) във вида

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_{13}x + 2a_{23}y + a_{33} = 0, \tag{5.1}$$

където $a_{ij} \in \mathbb{Z}$.

С линейни трансформации подобни на използваните при канонизация на коничните сечения в аналитичната геометрия уравнение (5.1) се свежда към

$$X^2 + 2aY + b = 0 \qquad \text{(парабола)}$$

или към

$$X^2 - DY^2 = F.$$

(Последното уравнение често се нарича уравнение на Пел, макар че Пел няма никакви приноси към неговото решаване.) Думите “свежда се” означават, че ако (5.1) има решение в цели числа, такова има и полученото уравнение. Но при връщане към изходното уравнение трябва да се внимава и това не винаги е възможно.

Нека $a_{11} = a_{22} = 0,\ a_{12} \neq 0$. Полагайки

$$\left| \begin{array}{lcl} x & = & u+v \\ y & = & u-v \end{array} \right.$$

получаваме

$$2a_{12}(u^2 - v^2) + 2(a_{13} + a_{23})u + 2(a_{13} - a_{23})v + a_{33} = 0.$$

Умножаваме полученото равенство по $2a_{12}$ и то добива вида

$$(2a_{12}u + a_{13} + a_{23})^2 - (2a_{12}v - a_{13} + a_{23})^2 + a_{33} - 4a_{13}a_{23} = 0.$$

С трансформацията

$$\left| \begin{array}{lcl} X & = & 2a_{12}u + a_{13} + a_{23} \\ Y & = & 2a_{12}v - a_{13} + a_{23} \end{array} \right. ,$$

то добива вида

$$X^2 - Y^2 = F.$$

(т.е. хипербола.)

Нека за конкретност $a_{11} \neq 0$. Тогава умножавайки (5.1) с a_{11} и полагайки

$$\left| \begin{array}{lcl} u & = & a_{11}x + a_{12}y \\ v & = & y \end{array} \right.$$

получаваме

$$u^2 + \Delta v^2 + 2a_{13}u + 2(a_{11}a_{23} - a_{12}a_{13})v + a_{11}a_{33} = 0,$$

където $\Delta = a_{11}a_{22} - a_{12}^2$.

Ако $\Delta \neq 0$, то умножавайки по Δ уравнението се преобразува в

$$\Delta(u + a_{13})^2 + (\Delta v + a_{11}a_{23} - a_{12}a_{13})^2 + \Delta[a_{11}a_{33} - a_{13}^2 - (a_{11}a_{23} - a_{12}a_{13})^2] = 0.$$

Сега полагането

$$\left| \begin{array}{lcl} X & = & \Delta v + a_{11}a_{23} - a_{12}a_{13} \\ Y & = & u + a_{13} \end{array} \right. ,$$

получаваме уравнение на Пел:

$$X^2 + \Delta Y^2 = F.$$

Да отбележим, че ако $a_{12} = 0$, то направо прилагаме последната стъпка с тази разлика, че умножаваме с $a_{11}a_{22}$ (което е пак Δ).

Нека $\Delta = 0$. С трансформацията

$$\left| \begin{array}{lcl} u & = & X - a_{13} \\ v & = & Y \end{array} \right. ,$$

то се преобразува в

$$X^2 + 2(a_{11}a_{23} - a_{12}a_{13})Y + a_{11}a_{33} - a_{13}^2 = 0.$$

Следователно случаят $\Delta = 0$ води до парабола и връзката между X, Y и първоначалните неизвестни x, y се дава с

$$\left| \begin{array}{rcl} a_{11}x & = & X - a_{12}Y - a_{13} \\ y & = & Y \end{array} \right. . \tag{5.2}$$

Да разгледаме параболичния случай по-подробно. Съществуването на решение в цели числа на $X^2 + 2aY + b = 0$ влече решимост на сравнението

$$X^2 \equiv -b \pmod{2a}. \tag{5.3}$$

За всяко решение X на (5.3) двойката цели числа X, Y, където $Y = (X^2 + b)/2a$ е решение на параболичното уравнение. Необходимото и достатъчно условие за решимост на сравнението (5.3) се дава с Теорема 4.1.10.

Пример 5.1.1 Да решим уравнението

$$x^2 - 2xy + y^2 - x - 2y = 0.$$

Следвайки описаната по-горе процедура го преобразуваме в

$$(x-y)^2 + 2(x-y) - 3x = 0,$$

откъдето полагайки

$$\left| \begin{array}{lcl} X & = & x \\ Y & = & x - y + 1 \end{array} \right.$$

получаваме

$$Y^2 - 3X - 1 = 0.$$

последното уравнение има решение в цели числа тогава и само тогава, когато е решимо сравнението

$$Y^2 \equiv 1 \pmod 3,$$

т.е. за $Y = 3t \pm 1,\ t \in \mathbb{Z}$. Следователно решенията му се дават с

$$X = 3t^2 + 2t, \qquad Y = 3t + 1$$

$$X = 3t^2 - 2t, \qquad Y = 3t - 1.$$

Използвайки връзката между старите и новите променливи получаваме решенията на първоначалното уравнение:

$$\begin{array}{ll} x = 3t^2 + 2t, & y = 3t^2 - t \\ x = 3t^2 - 2t, & y = 3t^2 - 5t + 2 \end{array}, \quad t \in \mathbb{Z}.$$

Пример 5.1.2 Да решим уравнението

$$xy - 2x + 3y - 1 = 0.$$

Съгластно дадената по-горе процедура това уравнение трябва да се преобразуваме в хипербола (в случая изродена в две пресичащи се прави). Полагайки $x = u+v$ и $y = u-v$ получаваме

$$u^2 - v^2 + u - 5v - 1 = 0. \tag{5.4}$$

След умножение по 4 се преобразува в

$$(2u+1)^2 - (2v+5)^2 + 20 = 0,$$

т.е. в

$$X^2 - Y^2 = -20, \tag{5.5}$$

където

$$\left| \begin{array}{lcl} X & = & 2u+1 \\ Y & = & 2v+5 \end{array} \right.$$

Уравнение (5.5) можем да запишем във вида

$$(X+Y)(X-Y) = -20.$$

Като вземем предвид, че $(X+Y)$ и $(X-Y)$ са с еднаква четност и решенията се групират по четворки като във всяка група има решение с $X \geq 0,\ Y \geq 0$, то решенията на (5.5) се получават от

$$\left| \begin{array}{ll} X+Y & = 10 \\ X-Y & = -2 \end{array} \right. , \qquad \left| \begin{array}{ll} X+Y & = 2 \\ X-Y & = -10 \end{array} \right. .$$

Следователно

$$\begin{array}{llll} X=4 & X=4 & X=-4 & X=-4 \\ Y=6 & Y=-6 & Y=6 & Y=-6 \end{array}$$

Използвайки връзката

$$\left| \begin{array}{lcl} X & = & x+y+1 \\ Y & = & x-y+5 \end{array} \right.$$

между старите и новите променливи получаваме решенията на първоначалното уравнение:

$$\begin{array}{llll} x=2 & x=-4, & x=-2 & x=-8 \\ y=1 & y=7 & y=-3 & y=3 \end{array} .$$

Забележка 5.1 *Горният пример е интересен и с това, че междинното уравнение (5.4) няма решение в цели числа (с проверка по модул 2 се вижда), но първоначалното и крайното уравнения (5.4) имат. С това напомняме, че преобразуванията не водят към еквивалентни диофантови уравнения и трябва да се внимава с изводите.*

5.2 Уравнения от вида $\mathbf{x^2 - Dy^2 = F}$.

Да отбележим първо, че ако (x_0, y_0) е решение на

$$x^2 - Dy^2 = F,$$

то $(x_0, -y_0)$, $(-x_0, y_0)$ и $(-x_0, -y_0)$ също са решения. Решенията с $x > 0,\ y > 0$ ще наричаме *положителни*, а такива, за които $y = 0$ или $x = 0$ (ако има такива) – *тривиални*.

Ако $D < 0$, то уравнението има вида

$$x^2 + \Delta y^2 = F, \quad \Delta > 0$$

и очевидно има най-много краен брой решения (елиптичен случай).

Ако D е точен квадрат, то уравнението се свежда към линейни диофантови уравнение (виж Пример 7.1.2). Затова предполагаме, че D не е точен квадрат на естествено число.

И така интересуваме се от случая, когато $D > 1$ е естествено число, което не е точен квадрат.

Лема 5.2.1 *Ако α е ирационално число, то съществуват безброй много двойки цели числа $(a, b) = 1$, такива че*

$$\left|\frac{a}{b} - \alpha\right| < \frac{1}{b^2}.$$

Доказателство. Да разделим интервала $[0, 1)$ на n равни части:

$$[0,1) = \cup \left[\frac{k}{n}, \frac{k+1}{n}\right),\ k = 0, 1, \ldots, n-1.$$

Тъй като α е ирационално, то дробните части на $0, \alpha, 2\alpha, \ldots, n\alpha$ са различни и следователно съществуват k и l, такива че дробните части на $k\alpha$ и $l\alpha$ попадат в един интервал, т.е. $0 \leq k < l \leq n$ и

$$|k\alpha - \lfloor k\alpha \rfloor - (l\alpha - \lfloor l\alpha \rfloor)| < \frac{1}{n}.$$

С полагането $a = \lfloor l\alpha \rfloor - \lfloor k\alpha \rfloor$ и $b = l - k < n$, неравенството добива вида

$$|a - b\alpha| < \frac{1}{n}.$$

Считаме, че a и b са взаимнопрости, тъй като в противния случай ще разделим неравенството на най-големия им общ делите, което само ще го усили. Освен това $b > 0$ влече

$$\left|\frac{a}{b} - \alpha\right| < \frac{1}{bn} < \frac{1}{b^2}.$$

Оставяйки n да расте получаваме различни двойки. Наистина, за всяка намерена двойка a, b избирайки n :

$$\frac{1}{n} < \left|\frac{a}{b} - \alpha\right|$$

и повтаряйки горните разсъждения получаваме c, d, такива че

$$\left|\frac{c}{d} - \alpha\right| < \frac{1}{dn} < \left|\frac{a}{b} - \alpha\right|.$$

Лема 5.2.2 *Ако D е естествено, което не е точен квадрат, то съществуват безброй много двойки естествени числа (a, b), такива че*

$$\left|a^2 - Db^2\right| < 1 + 2\sqrt{D}.$$

Доказателство. Числото $\sqrt{D} > 1$ е ирационално и съгласно предната лема съществуват безброй много двойки (в случая) естествени числа $(a, b) = 1$, за които

$$\left|a - b\sqrt{D}\right| < \frac{1}{b}.$$

Тогава

$$\left|a + b\sqrt{D}\right| \leq \left|a - b\sqrt{D}\right| + 2b\sqrt{D} < \frac{1}{b} + 2b\sqrt{D}.$$

Следователно

$$\left|a^2 - Db^2\right| = \left|a - b\sqrt{D}\right| \left|a + b\sqrt{D}\right| < \frac{1}{b^2} + 2\sqrt{D} < 1 + 2\sqrt{D}.$$

Теорема 5.2.3 *Ако D е естествено, което не е точен квадрат, то уравнението*

$$x^2 - Dy^2 = 1 \tag{5.6}$$

има безброй много решения в цели числа. При това съществува двойка естествени числа (x_1, y_1), които са решение на уравнението и всяко друго решение има вида $(\pm x_n, \pm y_n)$, където

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n.$$

Доказателство. Да отбележим, че от горната формула се получава при $n = 0$ формално и тривиалното решение (1,0).

От Лема 5.2.2 и $3 < 1 + 2\sqrt{D} < \infty$ следва, че съществува поне едно цяло число m, за което уравнението

$$x^2 - Dy^2 = m$$

се удовлетворява за безброй много двойки естествени числа. Но тъй като $|m|$ е крайно, то съществуват поне две такива двойки (x_1, y_1) и (x_2, y_2), такива че

$$x_1 \equiv x_2, \quad y_1 \equiv y_2 \pmod{|m|}.$$

Тогава

$$\begin{aligned}(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) &= (x_1x_2 - y_1y_2D) + (x_1y_2 - x_2y_1)\sqrt{D} \\ &\equiv (x_1^2 - Dy_1^2) + 0.\sqrt{D} \equiv 0 \pmod{|m|}.\end{aligned}$$

Следователно съществуват цели числа u, v :

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = m(u + v\sqrt{D})$$

и

$$(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) = m(u - v\sqrt{D}).$$

Умножавайки ги почлено получаваме

$$m^2 = m^2(u^2 - v^2D),$$

откъдето

$$u^2 - v^2D = 1.$$

Да отбележим, че $v \neq 0$. Наистина, противното води до $u = \pm 1$ и $x_1 y_2 = x_2 y_1$. Тогава умножавайки $x_1 x_2 - y_1 y_2 D = m(\pm 1)$ с x_1 получаваме:

$$\pm m x_1 = x_1^2 x_2 - y_1 x_1 y_2 D = x_1^2 x_2 - y_1^2 x_2 D = (x_1^2 - y_1^2 D) x_2 = m x_2.$$

Следователно $x_1 = x_2$ (те са естествени числа), което противоречи на избора им. С това доказахме съществуването на положително решение.

За да докажем второто твърдение въвеждаме наредба сред положителните решения. Казваме, че $(a,b) > (c,d)$, ако $a + b\sqrt{D} > c + d\sqrt{D}$. Нека $\alpha = u + v\sqrt{D}$ и $\beta = x + y\sqrt{D}$, където (u,v) е минималното положително, а (x,y) е произволно положително решение. Да отбележим, че $\bar{\alpha} = u - v\sqrt{D} = \alpha^{-1}$, тъй като$u^2 - v^2 D = 1$. Аналогично $\bar{\beta} = \beta^{-1}$. Нека n е такова естествено число, че $\alpha^n \leq \beta < \alpha^{n+1}$. Тогава $1 \leq (\bar{\alpha})^n \beta < \alpha$. Ако $(\bar{\alpha})^n \beta = a + b\sqrt{D}$, то $a - b\sqrt{D} = (a + b\sqrt{D})^{-1}$ и следователно $a^2 - b^2 D = 1$, т.е. (a,b) е решение на разглежданото уравнение. Но $1 \leq a + b\sqrt{D} < \alpha$, което влече $0 < a - b\sqrt{D} \leq 1$ и следователно $2a > 1$ и $2b\sqrt{D} \geq 1 - 1 = 0$. Следователно $a > 0$ и $b \geq 0$. В такъв случай единствената възможност да не сме в противоречие с избора на α (минимално положително решение) е $b = 0, a = 1$, т.е. $\alpha^n = \beta$.

Да отбележим, че ако (u,v) е решение на (5.6) и (a,b) е решение на

$$x^2 - Dy^2 = F, \tag{5.7}$$

то двойката (c,d) зададена с

$$(c + d\sqrt{D}) = (a + b\sqrt{D})(u + v\sqrt{D})$$

е също решение на (5.7). Това ни позволява да дадем следната

Дефиниция 5.2.4 *Нека D е естествено число, което не е точен квадрат и F е ненулево цяло число. Казваме, че две решения (a,b) и (c,d) на (5.7) са **асоциирани**, ако съществува решение (u,v) на (5.6), такова че*

$$(c + d\sqrt{D}) = (a + b\sqrt{D})(u + v\sqrt{D}).$$

Лесно се проверява, че горната дефиниция задава релация на еквивалентност в съвкупността от решения на (5.7). Следователно дясната страна на горното равенство е също решение на (5.7) и всички негови решения се разбиват на непресичащи се *класове от асоциирани решения.* Съгласно дадената дефиниция, ако (a,b) и (c,d) са асоциирани, то

$$(c + d\sqrt{D})(a - b\sqrt{D}) = F.(u + v\sqrt{D}).$$

Обратно, ако последното е в сила, то

$$(c - d\sqrt{D})(a + b\sqrt{D}) = F.(u - v\sqrt{D}),$$

откъдето с умножаване получаваме $u^2 - Dv^2 = 1$. Следователно (a,b) и (c,d) са асоциирани тогава и само тогава, когато

$$\left| \begin{array}{lcll} ac - bdD & \equiv & 0 & \pmod{F} \\ ad - bc & \equiv & 0 & \pmod{F}, \end{array} \right. \tag{5.8}$$

Класът с представител $a-b\sqrt{D}$ се нарича *спрегнат* на този с представител $a+b\sqrt{D}$. Ако двата класа съвпадат казваме, че класът е *самоспрегнат*. При $F=\pm 1$ има само един клас и той е самоспрегнат. Да отбележим, че в един клас може да има решение с $a=0$ или $b=0$, само ако класът е самоспрегнат. Затова, ако класът не е самоспрегнат може да изберем измежду всички решения онова, за което b приема минимална положителна стойност. Тогава съответното a е еднозначно определено, тъй като $(-a,b)$ принадлежи на спрегнатия клас, и $|a|$ също има минималната възможна положителна стойност. Така определеното (еднозначно) решение (a_0,b_0) наричаме *фундаментално решение (представител) за класа* .

В сила е следната теорема

Теорема 5.2.5 *Ако D и F са естествени числа и D не е точен квадрат, то уравненията*

$$x^2-Dy^2=\pm F \tag{5.9}$$

имат краен брой класове решения. При това, ако (u,v) е решение на (5.6), то

$$0<|x|\le\sqrt{\frac{(u\pm 1)D}{2}}$$

$$0\le y\le\frac{v}{\sqrt{2(u\pm 1)}}\sqrt{D}.$$

Фундаменталното решение на (5.6) може да се получи чрез развиване на $\sqrt{D}$ във безкрайна верижна дроб. Съгласно Теорема 1.5.8 тя се явява периодична и ако периодът ѝ $n+1$ е четно число, то числителят и знаменателят на $n-$тата ѝ приближена дроб $\dfrac{P_n}{Q_n}$ удовлетворяват

$$P_n^2-Q_n^2D=1$$

Ако $n+1$ е нечетно, то вземаме приближената дроб съответсваща на края на втория период, т.е. решението е (P_{2n+1},Q_{2n+1}).

Пример 5.2.1 Да решим уравнението

$$5x^2-14xy+7y^2+28x-28y+23=0.$$

Следвайки описаната в предния параграф процедура го умножаваме с 5 и преобразуваме във вида

$$(5x-7y)^2-14y^2+28(5x-7y)+56y+115=0,$$

откъдето с полагане

$$\left|\begin{array}{lcl} u & = & 5x-7y \\ v & = & y \end{array}\right.$$

получаваме

$$u^2-14v^2+28u+56v+115=0.$$

Последното записваме като

$$(u^2+28u+14^2)-14(v^2-4v+4)-25=0.$$

Като положим

$$\left|\begin{array}{lcl} X & = & u+14 \\ Y & = & v-2 \end{array}\right.$$

получаваме

$$X^2 - 14Y^2 = 25. \tag{5.10}$$

Едно очевидно решение е $(\pm 5, 0)$, което води до решенията $(5t, 5s)$, където (t, s) е произволно решение на

$$X^2 - 14Y^2 = 1. \tag{5.11}$$

Да намерим сега фундаменталното решение на (5.11) и след това да се опитаме да потърсим и други класове решения на (5.10). За целта да развием първо $\sqrt{14}$ във верижна дроб. Съгласно Пример 1.5.1

$$\sqrt{14} = [3; 1, 2, 1, 6, 1, 2, 1, 6, \ldots]$$

а за приближените дроби имаме:

$$\begin{array}{llllll} P_{-1} = 1, & P_0 = 3, & P_1 = 4, & P_2 = 11, & P_3 = 15, & \ldots \\ Q_{-1} = 0, & Q_0 = 1, & Q_1 = 1, & Q_2 = 3, & Q_3 = 4, & \ldots \end{array}$$

Двойката (P_3, Q_3) трябва да даде фундаменталното решение и наистина

$$15^2 - 14.4^2 = 1.$$

Следователно всяко положително решение на (5.11) се дава от

$$(15 + 4\sqrt{14})^n,\ n = 0, 1, 2, \ldots\ . \tag{5.12}$$

Съгласно Теорема 5.2.5 фундаменталните представители на класовете решения удовлетворяват

$$0 < |x| \le \sqrt{\frac{(15+1).14}{2}} = 4\sqrt{7} \qquad \text{и} \qquad 0 \le y \le \frac{4}{\sqrt{2(15+1)}}\sqrt{14} = \sqrt{7},$$

т. е.

$$0 < |x| \le 10 \qquad \text{и} \qquad 0 \le y \le 2.$$

Проверката в (5.10) със стойности в посочените граници дава още два класа решения: $(9, 2)$ и $(9, -2)$. Те водят до решения

$$(9t + 28s,\ 2t + 9s) \quad \text{и} \quad (9t - 28s,\ -2t + 9s),$$

където (t, s) е решение на (5.11). Първите стойности са (247,66) и (23,6).

Връзката с началните променливи се дава с

$$\left|\begin{array}{rcl} 5x & = & X + 7Y \\ y & = & Y + 2 \end{array}\right. ,$$

откъдето получаваме

$$\begin{array}{lll} x = t + 7s & 5x = 23t + 91s & x = -t + 7s \\ y = 5s + 2 & y = 2t + 9s + 2 & y = -2t + 9s + 2 \end{array} .$$

Тъй като (виж (5.12)) точно едно от t и s във всяка двойка е кратно на 5, то $23t+91s \not\equiv 0 \pmod 5$. Следователно решенията на първоначалното уравнение се дават само с

$$\begin{array}{ll} x = t + 7s & x = -t + 7s \\ y = 5s + 2 & y = -2t + 9s + 2 \end{array},$$

където (t,s) е решение на (5.11). Например решения са $(1,2),\ (-1,0),\ (1,4),\ (13,8)$.